

# HIDDEN SYMMETRIES AND $j(\tau)$

K. M. BUGAJSKA

**ABSTRACT.** We show that, for supersingular prime  $p$ , the image of a unique meromorphic function  $G_p$  on  $X_0(p)$  (of the degree two, with the polar divisor  $\{[0]_0, [\infty]_0\}$ ) under a certain Hecke operator is equal to  $j(\tau)$  (up to some additive constant). This generates quantities of relations between the coefficients of  $j(\tau)$  and leads to some group of hidden symmetries whose order must be divided by  $p$ .

## 1. INTRODUCTION

Let  $R_p$  denote a fundamental domain of  $\Gamma_0(p)$  which for  $p \geq 3$  is given as

$$R_p = R \cup \bigcup_{m=-\frac{p-1}{2}}^{\frac{p-1}{2}} \beta_m R, \quad \beta_m = ST^m, \quad S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

Here  $R$  is the standard quadrilateral fundamental domain for  $\Gamma = SL_2\mathbb{Z}$  in the upper half-plane  $H$  i.e.

$$R = \{\tau \in H; |\tau| \geq 1, -1 \leq \operatorname{Re}\tau \leq 0\} \cup \{\tau \in H; |\tau| > 1, 0 < \operatorname{Re}\tau < 1\}$$

We choose the domain  $R_p$  because the imaginary axis is its symmetry axis and this makes the visualization of the appropriate pairs of the Weierstrass points on  $X_0(p)$  much easier. By  $\mathcal{P}_S$  we will denote the set of all supersingular primes  $\{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 41, 47, 59, 71\}$ . They have the property that the genus of  $H^*/\Gamma_0^+(p)$  is zero which implies that the modular curve  $X_0(p)$  is hyperelliptic with the hyperelliptic involution given by the Fricke involution  $\omega_p = \begin{pmatrix} 0 & 1 \\ -p & 0 \end{pmatrix}$

acting on the upper halfplane  $H$  (i.e.  $\hat{\omega}_p = \frac{1}{\sqrt{p}}\omega_p = \begin{pmatrix} 0 & \frac{1}{\sqrt{p}} \\ -\sqrt{p} & 0 \end{pmatrix} \in SL_2\mathbb{R}$ ). The curve  $X_0(37)$  is also hyperelliptic however, it was shown by Ogg in [1], that its hyperelliptic involution  $v$  is an exceptional one i.e. it is not determined by  $\hat{\omega}_p$ .

We start with showing that, for any prime  $p \geq 3$ , each stable point of  $\hat{\omega}_p : X_0(p) \rightarrow X_0(p)$  determines an ideal class  $\kappa$  in  $\mathcal{C}\mathcal{O}_{\mathcal{K}}$  or in  $\mathcal{C}\mathcal{O}_{\mathcal{K}} \cup \mathcal{C}\mathcal{O}$  (depending whether  $p$  is congruent to 1 or to 3 modulo 4 respectively,  $\mathcal{K} = \mathbb{Q}(\sqrt{-p})$ ), and conversely, any such class  $\kappa$  determines a unique ramification point of  $\pi_{\omega} : X_0(p) \rightarrow \Sigma = X_0(p)/\hat{\omega}_p$ . Hence, the class numbers and the Gauss conjecture restricted to primes may be expressed (see (5.4)) in terms of the genus  $g$  of  $X_0(p)$  and the genus  $\gamma$  of  $\Sigma$  using the Riemann-Hurwitz theorem. It makes possible to look for the properties of the class groups by investigating the properties of the ramification points of  $\pi_{\omega}$  on  $X_0(p)$ .

---

*Date:* December 14, 2010.

*2010 Mathematics Subject Classification.* Primary 30F99; Secondary 08A99.

When  $\gamma = 0$ , (i.e. when  $p \in \mathcal{P}_S$ ) then the curve  $X_0(p)$  must carry a unique meromorphic function  $G_p$  that is invariant under  $\tilde{\omega}_p$ , has polar divisor  $G_p^\infty = \{[0]_0, [\infty]_0\}$  and is normalized such that its lifting  $G_p(\tau)$  to  $H$  has the coefficient by  $q^{-1}$  (in the Fourier expansion about  $i\infty$ ) equal to one. When  $X_0(p)$  has genus zero itself then  $G_p(\tau)$  is expressed in terms of the absolute invariant  $\Phi_p(\tau)$ , (3.1), for  $\Gamma_0(p)$ . Next we use the Hecke operators  $[\Gamma_0(p)\omega_p\Gamma]_0$ , [2], to transform the  $\Gamma_0^+(p)$ -invariant functions  $G_p(\tau)$  into  $\Gamma$ -invariant functions  $P_p(\tau)$ . It appears that, up to a constant given by the value  $P_p(\rho)$ , functions  $j(\tau)$  and  $P_p(\tau)$  coincide. Now, the construction of  $P_p(\tau)$  out of  $G_p(\tau)$  provides important relations between the coefficients  $c_n$  of  $j(\tau)$  which are investigated in sections 3 and 4. It seems that all this leads to some group of hidden symmetries whose order must be divided by  $p$ .

On the other hand, the fact that all  $c_n$ 's are integers imply that for some super-singular primes  $p$  and for positive integers  $m \notin (p)$  we may have pure non-rational  $(p, m)$ -absolute constants. When  $\Omega_n^p = \Omega_m^p$  for  $m, n \notin (p)$ ,  $m \neq n$  then we may have an absolute (not rational)  $p$ -invariant. (When genus of  $X_0(p)$  is zero than all  $\Omega_n^p = 0$ .)

We easily notice that when we consider relations between the coefficients for all singular primes simultaneously then the gigantic number of relations, their complexity and character as well as the relation (3.18) may indicate an occurrence of some vertex algebra.

At the end we list emerging open (to the author's knowledge) questions.

## 2. WEIERSTRASS POINTS AND CLASS GROUPS

Let  $p$  be an odd prime. For any  $\tau \in H$  we denote by  $[\tau]_0$  the class  $\Gamma_0(p)\tau$  and by  $[\tau]$  the set  $\Gamma\tau$ . Let  $\tilde{\omega}_p : X_0(p) \rightarrow X_0(p)$  be the map induced by the Fricke involution  $\omega_p = \begin{pmatrix} 0 & 1 \\ -p & 0 \end{pmatrix}$  acting on  $H$  and let  $\mathfrak{B}_p = (b_1, \dots, b_B)$  be the set of the stable points of  $\tilde{\omega}_p$  and hence the set of the ramification points of the mapping  $\pi_\omega : X_0(p) \rightarrow \Sigma$  where  $\Sigma \cong H/\Gamma_0^+(p) \cong X_0(p)/\tilde{\omega}_p$ .

An element  $[\tau]_0 \in X_0(p)$  belongs to  $\mathfrak{B}_p$  if and only if we have  $\omega_p\tau = A\tau$  for some  $A = \begin{pmatrix} a & b \\ kp & d \end{pmatrix} \in \Gamma_0(p)$  (without a loss of generality we may assume that  $a > 0$ ). Since  $\tau_0 = \frac{i}{\sqrt{p}}$  satisfies  $\omega_p\tau_0 = \tau_0$  we have  $[\tau_0]_0 \in \mathfrak{B}_p$ . For other elements,  $\tau$  must be a solution of

$$(2.1) \quad ap\tau^2 + (bp + kp)\tau + d = 0$$

and hence we must have  $A = \begin{pmatrix} a & b \\ bp & d \end{pmatrix}$  and  $\tau = \frac{1}{a}(\tau_0 - b)$ . When  $b = 1$  and  $a = 2$  we obtain  $\tau_1 = \frac{1}{2}(\tau_0 - 1)$ . It represents the same element of  $X_0(p)$  as the  $\tau$  obtained when  $b = -1$ . However for  $a > 2$  this is no longer true. In this case we obtain the pair of elements  $\tau_\pm = \frac{1}{a}(\tau_0 \mp b)$ ,  $b > 0$  (with corresponding matrices  $A_\pm = \begin{pmatrix} a & \pm b \\ \pm b & \frac{pb^2+1}{a} \end{pmatrix}$ ) such that their classes  $[\tau_+]_0$  and  $[\tau_-]_0$  represent distinct points of  $\mathfrak{B}_p$ .

Let  $\mathcal{K} = \mathbb{Q}(\sqrt{-p})$ , let  $\mathcal{O}_{\mathcal{K}} = [1, \beta_{-p}]$  denotes its ring of integers and let  $\mathcal{O} = [1, 2\beta_{-p}]$  denote its order with conductor 2, (here  $\beta_{-p} = \sqrt{-p}$  when  $p \equiv 1 \pmod{4}$  and  $\beta_{-p} = \frac{1+\sqrt{-p}}{2}$  when  $p \equiv 3 \pmod{4}$ ). Let  $u$  denote the reduce number of  $\tau$ , that is, a unique element of the standard fundamental domain  $R$  of  $SL_2\mathbb{Z}$  such that  $[u] = [\tau]$ .

**Lemma 1.** *For odd primes each ramification point  $[\tau]_0 \in \mathfrak{B}_p \subset X_0(p)$  corresponds to a unique class  $\kappa \in \text{Cl}\mathcal{O}_K$  when  $p \equiv 1 \pmod{4}$  or to  $\kappa \in \text{Cl}\mathcal{O}_K \cup \text{Cl}\mathcal{O}$  when  $p \equiv 3 \pmod{4}$*

*Proof.* First we notice that  $[\tau_0] = [\sqrt{-p}]$  determines the class of the ideal  $[1, \beta_{-p}]$  in  $\text{Cl}\mathcal{O}_K$  for  $p \equiv 1 \pmod{4}$  and the class of  $[1, 2\beta_{-p}]$  in  $\text{Cl}\mathcal{O}$  for  $p \equiv 3 \pmod{4}$ . Now  $u_0 = S\tau_0 = \sqrt{-p}$  is the reduced number representing this class. The class  $[\tau_1] = [u_1]$  of  $\Gamma$ -equivalent elements ( $u_1 = \frac{1}{2}(u_0 - 1)$ ) always determines a class in  $\text{Cl}\mathcal{O}_K$ . For other stable points of  $\tilde{\omega}_p$  we may use the fact that when the  $\gcd(ap, 2bp, d) = 1$  then the discriminant of a solution of (2.1) is  $D(\tau) = -4p$  and hence it coincides with the discriminant  $\Delta_K$  for  $p \equiv 1 \pmod{4}$  or with the discriminant  $\Delta_{\mathcal{O}}$  when  $p \equiv 3 \pmod{4}$ . When  $\gcd(ap, 2bp, d) = l > 1$  then we must have that  $l = 2$  and  $D(\tau) = -p$ . This occurs only when  $p \equiv 3 \pmod{4}$  and then we have  $D(\tau) = \Delta_K$ .  $\square$

**Lemma 2.** *Each class  $\kappa \in \text{Cl}\mathcal{O}_K$  for  $p \equiv 1 \pmod{4}$  and each class  $\kappa \in \text{Cl}\mathcal{O}_K \cup \text{Cl}\mathcal{O}$  for  $p \equiv 3 \pmod{4}$  contains an ideal  $\mathfrak{a} = [1, \tau]$  such that  $\omega_p \tau = A\tau$  for some  $A \in \Gamma_0(p)$ . Moreover, all ideals  $\mathfrak{a}$ 's with the property above which represent a given class  $\kappa$  are given by the elements  $\tau$ 's which belong to a unique  $\Gamma_0(p)$ -class  $[\tau]_0$ .*

*Proof.* We use the fact that the multiplicity of the class polynomial

$$(2.2) \quad \mathcal{H}_p(X) = \prod_{\kappa \in \text{Cl}\mathcal{O}_K} (X - j(\kappa)) \in \mathbb{Z}[X]$$

in the diagonal modular polynomial  $G_p(X) = F_p(X, X)$  (where  $F_p(X, j) = \prod_{k=0}^{p-1} (X - j \circ \alpha_k)$ ) is equal to one. The same is true when  $p \equiv 3 \pmod{4}$  for

$$(2.3) \quad \mathcal{H}_{\mathcal{O}} = \prod_{\kappa \in \text{Cl}\mathcal{O}} (X - j(\kappa)) \in \mathbb{Z}[X]$$

This means that for the (unique) reduced number  $u \in R$  representing a class  $\kappa$  there exists the unique correspondence  $\alpha \in \Delta_p^* = \bigcup_{k=0}^{p-1} \Gamma \alpha_k$  such that  $\alpha u = u$ .

Here  $\alpha_k = \begin{pmatrix} 1 & k \\ 0 & p \end{pmatrix}$  when  $k = 0, \dots, p-1$  and  $\alpha_p = \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}$ .

To prove our statement we must show that there exists a unique element  $\tau_m = \beta_m u \in \mathfrak{R}_p$ ,  $m \in \{-\frac{p-1}{2}, \dots, \frac{p-1}{2}\}$ ,  $\beta_m = \begin{pmatrix} 0 & 1 \\ -1 & -m \end{pmatrix} = ST^m$ , such that  $\omega_p \tau_m = A_m \tau_m$  for some  $A_m \in \Gamma_0(p)$ . The unique correspondence  $\alpha \in \Delta_p^*$  such that  $\alpha u_0 = u_0$  is  $\alpha = S\alpha_0 \in \Gamma\alpha_0$  and we have  $\tau_0 = \beta_0 u_0 \in \mathfrak{R}_p$ . Similarly it is easy to see that the class in  $\text{Cl}\mathcal{O}_K$  represented by  $[1, u_1]$  has the reduced number  $u_1 = \frac{1}{2}(u_0 + 1)$  that satisfies  $\alpha u_1 = u_1$  for unique correspondence  $\alpha \in \Gamma\alpha_{\frac{p-1}{2}}$ . Now  $\beta_{-\frac{p-1}{2}} u_1 = \omega_p \tau_1 \in \mathfrak{R}_p$  and it determines  $[\tau_1]_0 \in \mathfrak{B}_p$ . For the remaining cases, let an ideal  $[1, u]$  with  $u \in R$  represent a class  $\kappa$ , let  $\alpha = \gamma \alpha_m$  for some  $m$  and for some  $\gamma \in \Gamma$ , be the unique correspondence such that  $\alpha u = u$ . For each  $j \in \{-\frac{p-1}{2}, \dots, \frac{p-1}{2}\}$  and  $\tau_j = \beta_j u$  we have

$$\tilde{\alpha}_j \tau_j = \tau_j \quad \text{with} \quad \tilde{\alpha}_j = \beta_j \alpha \beta_j^{-1} \in \Delta_p^*$$

Since the multiplicity of the class polynomials in  $G_p(X)$  are equal to one all  $\tilde{\alpha}_j$  belong to distinct cosets of  $\Gamma$  in  $\Delta_p^*$  and hence there exists only one  $\tau_j$  such that  $\tilde{\alpha}_j \in \Gamma \alpha_p$  i.e. there is unique  $\tau_j$  such that  $\tilde{\alpha}_j = \gamma^{-1} \omega_p$  for some  $\gamma \in \Gamma$ . This means that

$$(2.4) \quad \omega_p \tau_j = \gamma \tau_j$$

| $p$         | 3 | 5 | 7 | 11 | 13 | 17 | 19 | 23 | 29 | 31 | 41 | 47 | 59 | 71 |
|-------------|---|---|---|----|----|----|----|----|----|----|----|----|----|----|
| $g(X_0(p))$ | 0 | 0 | 0 | 1  | 0  | 1  | 1  | 2  | 2  | 2  | 3  | 4  | 5  | 6  |
| $h_K$       | 1 | 2 | 1 | 1  | 2  | 4  | 1  | 3  | 6  | 3  | 8  | 5  | 3  | 7  |
| $h_2$       | 1 |   | 1 | 3  |    |    | 3  | 3  |    | 3  |    | 5  | 9  | 7  |
| $2g + 2$    | 2 | 2 | 2 | 4  | 2  | 4  | 4  | 6  | 6  | 6  | 8  | 10 | 12 | 14 |

We must show that  $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$  is in fact an element of  $\Gamma_0(p)$ . However, from (2.4),  $\tau_j$  is a solution of  $pa\tau^2 + (pb + c)\tau + d = 0$ . Since ideals  $[1, u]$  and  $[1, \tau_j]$  belong to the same class  $\kappa$  we have that  $D(\tau_j)$  is equal to  $-4p$  or to  $-p$  appropriately and this implies that  $\gamma \in \Gamma_0(p)$ . Hence, each class  $\kappa \in Cl\mathcal{O}_K$  for  $p \equiv 1 \pmod{4}$  and each class  $\kappa \in Cl\mathcal{O}_K \cup Cl\mathcal{O}$  for  $p \equiv 3 \pmod{4}$  is associated to a unique point of  $X_0(p)$  that is stable under  $\tilde{\omega}_p$ .  $\square$

**Corollary 1.** *There is a one-one correspondence between the set  $\mathfrak{B}_p$  of the ramification points of the projection  $\pi_\omega : X_0(p) \rightarrow \Sigma \cong X_0(p)/\tilde{\omega}_p$  and the set of elements of  $Cl\mathcal{O}_K$  for  $p \equiv 1 \pmod{4}$  or the set of elements of  $Cl\mathcal{O}_K \cup Cl\mathcal{O}$  when  $p \equiv 3 \pmod{4}$ .*

This means that, when a prime  $p$  belongs to  $\mathcal{P}_S$ , the number of elements in  $Cl\mathcal{O}_K$  or in  $Cl\mathcal{O}_K \cup Cl\mathcal{O}$  is determined exactly by the number of the Weierstrass points of  $X_0(p)$ . For a general prime  $p$  it is described by the Riemann-Hurwitz theorem (when the genus of  $\Sigma$  is greater than zero). In other words we have

$$(2.5) \quad |\mathfrak{B}_p| = h_K + h_2, \quad p \equiv 3 \pmod{4} \quad \text{and} \quad |\mathfrak{B}_p| = h_K, \quad p \equiv 1 \pmod{4}$$

where  $h_K = |Cl\mathcal{O}_K|$ ,  $h_2 = |Cl\mathcal{O}|$  and  $|S|$  denotes the cardinality of a set  $S$ .

When the genus of  $\Sigma = H/\Gamma_0^+(p)$  is zero then the Riemann surface  $X_0(p)$  is hyperelliptic with hyperelliptic involution corresponding to the Atkin-Lehner involution. Thus all points of  $\mathfrak{B}_p$  are exactly the  $2g + 2$  Weierstrass points on this surface. A set of representatives of these points, for  $p \geq 3$  contains  $\tau_0$ ,  $\tau_1$  and additional  $2g$  points when the genus of  $X_0(p)$  is  $g \geq 1$ . We may choose these points as given by

$$(2.6) \quad \tau_\pm = \frac{1}{a}(\tau_0 \mp b) \quad \text{with} \quad 0 < b < \frac{a}{2}, \quad 2 < a < 2\sqrt{\frac{p}{3}}$$

and hence the reduced numbers associated to points of  $\mathfrak{B}_p$  are given by

$$u_\pm = \frac{1}{a}(u_0 \pm 1) \quad \text{for} \quad b = 1, \quad u_\pm = \frac{1}{a}(u_0 \mp r) \quad \text{for} \quad a = br + 1, \quad b \geq 2$$

and

$$u_\pm = \frac{1}{a}(u_0 \pm r) \quad \text{for} \quad a = br - 1$$

The genus of  $X_0(p)$  is zero for  $p = 2, 3, 5, 7, 13$  and hence the set  $\mathfrak{B}_p$  for these primes contains only two points:  $\mathfrak{B}_p = \{[\tau_0]_0, [\tau_1]_0\}$  for  $p \neq 2$  and  $\mathfrak{B}_2 = \{[\frac{i+1}{2}]_0, [\frac{i}{\sqrt{2}}]_0\}$  (with the reduced numbers  $i$  and  $i\sqrt{2}$  respectively). For other primes in  $\mathcal{P}_S$  the elements  $\tau$ 's representing the remaining  $2g$ ,  $\tilde{\omega}_p$ -stable points of  $X_0(p)$ , may be easily found using the formulae (2.6). It is easy to determine which of these  $\tau$ 's represent an ideal class in  $Cl_K$  and which represents a class of  $Cl\mathcal{O}$ . We collect some results for the odd primes  $p \in \mathcal{P}_S$  in the table above.

3. FUNCTION  $P_p$ 

3.1. **A genus zero case.** When  $p = 2, 3, 5, 7, 13$  the genus of the modular curve  $X_0(p)$  is zero and the rational function field  $\mathbb{C}(X_0(p))$  is given by the absolute invariant

$$(3.1) \quad \Phi_p(\tau) = \left( \frac{\Delta(p\tau)}{\Delta(\tau)} \right)^{\frac{1}{p-1}} = \left( \frac{\eta(p\tau)}{\eta(\tau)} \right)^r, \quad r = \frac{24}{p-1}$$

that is  $\mathbb{C}(X_0(p)) = \mathbb{C}(\Phi_p(\tau))$ . The absolute invariant  $\Phi_p$  satisfies  $\Phi_p(\omega_p\tau) = p^{-\frac{r}{2}}\Phi_p^{-1}(\tau)$ , [3], and the series expansions of these functions at  $i\infty$  are:

$$(3.2) \quad \Phi_p(\tau) = q[1 + \sum_{n=1}^{\infty} b_n q^n], \quad b_n \in \mathbb{Z}, \quad q = e^{2\pi i\tau}$$

and

$$(3.3) \quad \Phi_p(\omega_p\tau) = p^{-\frac{r}{2}}[q^{-1} + \sum_{n=0}^{\infty} a_n q^n], \quad a_n \in \mathbb{Z}$$

Two points of  $X_0(p)$  that are stable under  $\tilde{\omega}_p$  are  $[\tau_0 = \frac{i}{\sqrt{p}}]_0$  and  $[\frac{1}{2}(\tau_0 - 1)]_0$  when  $p \neq 2$  or  $[\tau_1 = \frac{1}{2}(i-1)]_0$  when  $p = 2$ . Moreover we must have

$$\Phi_p(\tau_0) = -\Phi_p(\tau_1) \quad \text{with} \quad \Phi_p(\tau_i) = \pm p^{-\frac{r}{4}}, \quad i = 0, 1$$

Since the genus of  $X_0(p)/\tilde{\omega}_p$  is zero there exists a meromorphic function  $G_p$  of degree two on  $X_0(p)$  with the polar divisor  $\{\infty_1, \infty_2\} = \{[0]_0, [\infty]_0\}$  such that the following diagram commutes.

$$\begin{array}{ccc} X_0(p) & \xrightarrow{\tilde{\omega}_p} & X_0(p) \\ \downarrow G_p & \swarrow G_p & \\ \hat{\mathbb{C}} & & \end{array}$$

Diag.1

The lifting  $G_p(\tau)$  of the function  $G_p$  to  $H$  must satisfy

$$(3.4) \quad G_p(\omega_p\tau) = G_p(\tau), \quad G_p(\gamma\tau) = G_p(\tau), \quad \forall \tau \in H, \quad \forall \gamma \in \Gamma_0(p)$$

so the function  $G_p(\tau)$  is an automorphic function of  $\Gamma_0^+(p)$ . The polar divisor of  $G_p$  tells us that the series expansion of its lifting  $G_p(\tau)$  about  $i\infty$  is

$$(3.5) \quad G_p(\tau) = q^{-1} + G_p^+(q); \quad G_p^+(q) = \sum_{n=0}^{\infty} \alpha_n^p q^n$$

where we have normalized  $G_p(\tau)$  such that the coefficient by  $q^{-1}$  is one. We observe that the polar divisor of the function  $\Phi_p(\tau) + \Phi_p(\omega_p\tau)$  is the same as the polar divisor of  $G_p(\tau)$  and hence (3.2), (3.3) and (3.5) imply that

$$(3.6) \quad G_p(\tau) = p^{\frac{r}{2}}[\Phi_p(\tau) + \Phi_p(\omega_p\tau)] = q^{-1} + \sum_{n=0}^{\infty} \alpha_n^p q^n$$

with

$$(3.7) \quad \alpha_0 = a_0 = -b_1, \quad \alpha_1 = p^{\frac{r}{2}} + a_1, \quad \alpha_n = p^{\frac{r}{2}}b_{n-1} + a_n, \quad n \geq 2$$

Now, any  $\Gamma_0(p)$ -automorphic function determines a  $\Gamma$ -automorphic function by applying an appropriate Hecke operator. In other words, we will define the function  $P_p(\tau) \in \mathcal{A}_0(\Gamma) = \mathbb{C}(j)$  as the image of  $G_p(\tau)$  under the Hecke operator [2]

$$(3.8) \quad [\Gamma_0(p)\omega_p\Gamma]_0 : \mathcal{A}_0(\Gamma_0(p)) \rightarrow \mathcal{A}_0(\Gamma)$$

that is

$$(3.9) \quad P_p(\tau) = [\Gamma_0(p)\omega_p\Gamma]_0 G_p(\tau) = \sum_{k=0}^p G_p(\omega_p\gamma_k\tau) = \sum_{k=0}^p G_p(\gamma_k\tau)$$

where  $\omega_p\gamma_k = \begin{pmatrix} -1 & -k \\ 0 & -p \end{pmatrix}$  for  $k = 0, 1, \dots, p-1$  and  $\omega_p\gamma_p = \begin{pmatrix} 0 & -1 \\ p & 0 \end{pmatrix}$ . We may rewrite the last formula as

$$(3.10) \quad P_p(\tau) = G_p(\tau) + \sum_{k=1}^{p-1} G_p\left(\frac{\tau+k}{p}\right)$$

Using expansions (3.2) and (3.3) we obtain

$$(3.11) \quad P_p(\tau) = j(\tau) - j(\hat{u}_p) = q^{-1} + \alpha_0^p(p+1) + \sum_{n=1}^{\infty} (\alpha_n^p + p\alpha_{np}^p)q^n$$

where  $\hat{u}_p$  is the unique reduced number such that  $j(\hat{u}_p) = -P_p(\rho)$ . Thus we have

$$(3.12) \quad P_p(\tau) = j(\tau) + P_p(\rho) \quad \text{and} \quad P_p(\rho) = a_0^p(p-1) - 744$$

The vanishing of  $P_p(\tau)$  at  $\hat{u}_p \in R \subset R_p$  implies that we have

$$G_p(\hat{u}_p) = - \sum_{k=0}^{p-1} G_p\left(\frac{\hat{u}_p+k}{p}\right) = - \sum_{k=0}^{p-1} G_p(\gamma_k\hat{u}_p)$$

That means that the value of  $G_p$  at any one point of the set of  $p$  points on  $X_0(p)$  determined by  $\{\beta_k\hat{u}_p, k = \frac{-p+1}{2}, \dots, \frac{p-1}{2}\} \subset \mathfrak{R}_p$  is exactly the negative sum of the values of  $G_p$  at the remaining points.

We observe that using (3.10) and (3.11) we may view the absolute  $\Gamma$  invariant  $j(\tau)$  on its standard fundamental domain  $R$  as given (up to the additive constant  $P_p(\rho) = -j(\hat{u}_p)$ ) by the value of  $G_p(\tau)$  at  $\tau \in R$  plus the fundamental symmetric function  $\sigma_1(G_p(\gamma_0\tau), \dots, G_p(\gamma_{p-1}\tau))$  of the values of  $G_p(\tau)$  at all points that are  $\Gamma$ -equivalent to  $\tau \in R$  but represent all the remaining, distinct  $\Gamma_0(p)$ -classes.

**3.2. A genus  $g \geq 1$  case.** We have already mentioned that when the genus of  $X_0(p)$  is greater than two but the genus of  $X_0(p)/\tilde{\omega}_p$  is zero then  $X_0(p)$  must be a hyperelliptic Riemann surface (we recall that any surface of genus two is already a hyperelliptic one). The set  $\mathfrak{W}_p$  of  $2g+2$  Weierstrass points of  $X_0(p)$  coincides with the set  $\mathfrak{B}_p$  of the stable points of  $\tilde{\omega}_p : X_0(p) \rightarrow X_0(p)$  and with the set of elements of  $Cl\mathcal{O}_{\mathcal{K}}$  when  $p \equiv 1 \pmod{4}$  or with the set  $Cl\mathcal{O}_{\mathcal{K}} \cup Cl\mathcal{O}$  when  $p \equiv 3 \pmod{4}$ . Since we have found all Weierstrass points in the previous section we know that infinity is not one of them and hence we may introduce the function  $G_p$  as follows. Let  $G_p$  be a unique (up to multiplicative constant) a degree two meromorphic function on  $X_0(p)$  satisfying the properties of the commutative Diag.1 and whose polar divisor is  $\{\infty_1, \infty_2\} = \{[0]_0, [\infty]_0\}$ . Of course, its lifting  $G_p(\tau)$  to  $H$  satisfies the conditions

(3.4) for  $p = 11, 17, 19, 23, 29, 31, 41, 47, 59, 71$  and we normalize this function such that its Fourier expansion around  $i\infty$  has a form

$$(3.13) \quad G_p(\tau) = q^{-1} + \sum_{n=0}^{\infty} \alpha_n^p q^n, \quad q = e^{2\pi i \tau}$$

Similarly as in the genus zero case we use the Hecke operators  $[\Gamma_0(p)\omega_p\Gamma]_0$  to transform  $G_0(\tau) \in \mathcal{A}_0(\Gamma_0(p))$  into a  $\Gamma$ -invariant function

$$(3.14) \quad [\Gamma_0(p)\omega_0\Gamma]_0 G_p(\tau) = \sum_{m=0}^p G_p(\omega_p \gamma_m \tau) \in \mathcal{A}_0(\Gamma) = \mathbb{C}(j)$$

Similarly as before we will denote this image as  $P_p(\tau)$ . Thus we have

$$(3.15) \quad P_p(\tau) = G_p(\tau) + \sum_{k=-\frac{p-1}{2}}^{\frac{p-1}{2}} G_p(\beta_k \tau) = G_p(\tau) + \sum_{m=0}^{p-1} G_p\left(\frac{\tau+m}{p}\right)$$

whose Fourier expansion around  $i\infty$  is

$$(3.16) \quad P_p(\tau) = q^{-1} + \alpha_0^p(p+1) + \sum_{n=1}^{\infty} (\alpha_n^p + p\alpha_{np}^p) q^n \in \mathbb{C}(j)$$

We see immediately that

$$(3.17) \quad P_p(\tau) = j(\tau) + \text{const} \quad \text{with} \quad \text{const} = P_p(\rho)$$

There exists unique element  $\hat{u}_p$  in the fundamental domain  $R$  of  $\Gamma$  such that  $P_p(\rho) = -j(\hat{u}_p)$  and hence we may rewrite the last formula as

$$(3.18) \quad P_p(\tau) = j(\tau) - j(\hat{u}_p) = j(\tau) + P_p(\rho)$$

Hence

$$(3.19) \quad P_p(\hat{u}_p) = 0 \quad \text{and} \quad P_p(\rho) = \alpha_0^p(p+1) - 744$$

The first equality gives us

$$(3.20) \quad G_p(\hat{u}_p) = - \sum_{k=-\frac{p-1}{2}}^{\frac{p-1}{2}} G_p(\beta_k \hat{u}_p)$$

that is, the value of  $G_p(\tau)$  at  $\hat{u}_p$  is equal to the negative sum of the values of  $G_p(\tau)$  at the remaining points of  $R_p - R$  that are  $\Gamma$ -equivalent to  $\hat{u}_p$ . Now, from (3.16) and (3.18) we obtain

$$(3.21) \quad j(\tau) = P_p(\tau) + j(\hat{u}_p) = q^{-1} + 744 + \sum_{n=1}^{\infty} c_n q^n$$

and hence

$$(3.22) \quad 744 = \alpha_0^p(p-1) - P_p(\rho) \quad \text{and} \quad c_n = \alpha_n^p + p\alpha_{np}^p$$

## 4. HIDDEN SYMMETRIES

In the previous section we have found some relations between the coefficients  $c_n$  of  $j(\tau)$  (for  $n \geq 1$ ) and the coefficients  $\alpha_n^p$  of the  $\Gamma_0^+(p)$  invariant functions  $G_p(\tau)$ ,  $p \in \mathcal{P}_S$ . Namely, we have found that  $c_n = \alpha_n^p + p\alpha_{np}^p$ . Suppose that we know all functions  $G_p(\tau) = q^{-1} + \sum_{k=0}^{\infty} \alpha_k^p q^k$  (i.e. we know all  $\alpha_k^p$ 's). However, before we will investigate the consequences of these relations let us look at the  $p$ -decompositions of the positive integers for a fixed prime  $p$ . Let  $n = \sum_{i=0}^N a_i p^i \Leftrightarrow (a_0, a_1, \dots, a_N, 0, \dots)$  with all coefficients  $a_i \in \{0, 1, \dots, p-1\}$ . On  $\mathbb{Z}_{\geq 0}$  we may define the following two operations  $F_p$  and  $\sigma_p$  as given by

$$F_p(n) = pn \Leftrightarrow (0, a_0, \dots, a_N, 0, \dots) \quad \text{and} \quad \sigma_p(n) = (\overline{a_0 + 1}, a_1, \dots, a_N, 0, \dots)$$

where  $\overline{a_0 + 1} = (a_0 + 1) \bmod p$ . Thus, any positive integer  $n$  can be uniquely written as

$$n = \sigma_p^{a_0} \circ F_p \circ \sigma_p^{a_1} \circ F_p \circ \dots \circ F_p \circ \sigma_p^{a_N}(0)$$

Let us fix  $k > 0, 0 < l < p$ . The action of the commutator  $H_p^{k,l} := [F_p^k, \sigma_p^l]$  on  $n$  depends only on the value of  $n \bmod p$ . More precisely

$$H_p^{k,l}(n) = -l + (\overline{a_0 + l} - a_0)p^k$$

So, for example, for a positive  $n \in (p)$  we have

$$[F_p^k, \sigma_p^l](n) = l(p^k - 1) = (l-1)p^k + (p-1) \sum_{m=0}^{k-1} p^m \in \mathbb{Z}^+$$

and hence the operations  $H_p^{k,l}$  transfer any positive element of the ideal  $(p)$  into a positive integer out of the ideal. For all remaining positive integers with  $n \bmod p \neq 0$  the expression  $\overline{a_0 + l} - a_0$  is negative whenever  $a_0 + l \geq p$  and the  $H_p^{k,l}$  image of such  $n$  must also be negative. When  $(a_0 + l) < p$  then  $n$  has a positive image  $H_p^{k,l}(n) = l(p^k - 1)$  which is exactly the same for all integers  $n$ 's whose non-zero coefficient  $a_0$  satisfies  $(a_0 + l) < p$ . In all cases the image of  $n \in \mathbb{Z}^+$  is not in  $(p)$  i.e.  $H_p^{k,l}[\mathbb{Z}^+] \cap (p) = \emptyset$ .

For each  $n \in \mathbb{Z}^+$  the operations  $F_p^k$  produce an infinite sequence  $\mathcal{S}(n) := \{F_p^k(n), k \geq 0\}$  (which we will write horizontally). If  $n \notin (p)$  then the sequence  $\mathcal{S}(n)$  is maximal but for any  $m = p^r n \in (p)$  we have  $\mathcal{S}(m) \subset \mathcal{S}(n)$ .

Operation  $\sigma_p$  acting on  $\mathbb{Z}_{\geq 0}$  satisfies  $\sigma_p^p = Id$ . It connects the first terms of  $p$  distinct infinite horizontal  $F_p$ -sequences and at least  $p-1$  of them have to be maximal. For this reason we may view  $\sigma_p$  as a transformation that moves a sequence  $\mathcal{S}(n)$  with  $n \Leftrightarrow (a_0, a_1, \dots)$  into an  $F_p$ -sequence  $\mathcal{S}(t)$  with  $t \Leftrightarrow (\overline{a_0 + 1}, a_1, \dots, a_N, 0, \dots)$ . In this way after  $p$  steps we will return to our original sequence  $\mathcal{S}(n)$  (we will write such operation  $\sigma_p$  vertically). Thus we have arranged all non-negative integers in some sort of two dimensional "step" sequenses with the "hight" of each step equal to  $p$ . Actually, we merely expose the structure of the positive rational integers inside of the  $p$ -adic tree of the  $p$ -adic integers  $\mathbb{Z}_p$ .

Let us return to the coefficients  $c_n$  of  $j(\tau)$ . The formulae (3.11) and (3.22) imply that for each  $k \geq 1$  we have

$$(4.1) \quad p^{k-1}c_{p^{k-1}n} - p^{k-2}c_{p^{k-2}n} + \dots + (-1)^{k-1}c_n = p^k\alpha_{p^k n}^p + (-1)^{k-1}\alpha_n^p$$

This means that any infinite set of the coefficients  $c_n$ 's whose indexes belong to a horizontal, maximal  $F_p$ -sequence  $\mathcal{S}(m)$  of integers are uniquely determined by the



element  $c_m$ . We may introduce the operation  $f_p$  which corresponds to the operation  $F_p$  as follows:

$$(4.2) \quad f_p : c_n \rightarrow c_{pn}, \quad f_p(c_n) = c_{pn} = \frac{1}{p}c_n + (p\alpha_{p^2n}^p - \frac{\alpha_n^p}{p})$$

We see that for any  $p \in \mathcal{P}_S$  the coefficients of  $j(\tau)$  form some kind of a graded  $\mathbb{Z}/p\mathbb{Z}$  structure such that the operation  $f_p$  produces an infinite, horizontal  $f_p$ -sequences of coefficients whose all terms are determined by the first one. On the contrary to  $F_p$ , the operation  $\sigma_p$  does not induces any numerical formula between the coefficients  $c_n$  and  $c_{\sigma(n)}$ . However, when we write  $n = a_0 + m$ ,  $a_0 = n \bmod p$ , we may introduce the formal operation  $\hat{\sigma}_p$ ,  $\hat{\sigma}_p^p = Id$ , wich produces the following “path” of the length  $p$  of infinite  $f_p$ -sequences:

$$\{f_p^k(c_n)\}_{k=0}^\infty \xrightarrow{\hat{\sigma}_p} \{f_p^k(c_{\overline{(a_0+1)+m}})\}_{k=0}^\infty \xrightarrow{\hat{\sigma}_p} \dots \xrightarrow{\hat{\sigma}_p} \{f_p^k(c_n)\}_{k=0}^\infty$$

Since  $n = 0$  does not generate an infinite  $F_p$ -sequence,  $F_p(0) = 0$ , the same is true for  $c_0$ . This means that the role of the free coefficient  $c_0$  in  $j(\tau)$  is a distinguished one. In fact, the earlier obtained relations

$$c_0 = \alpha_0^p(p-1) - P_p(\rho) \quad \text{and} \quad j(\tau) = P_p(\tau) - P_p(\rho), \quad \tau \in H$$

tell us about some connection between  $c_0$  and the point  $\tau = \rho \in H$  that is associated to each  $p \in \mathcal{P}_S$ . It also tells us about a connection between the whole function  $j(\tau)$  and the torus determined by the lattice  $L_\rho$ . We have seen in [4] and [5] that this connection is very important and a.o. manifests itself by the production of a generating matrix for the binary error correcting Golay code  $G_{24}$  out of the properties of the Veech modular curve  $\mathbf{T}^* = H/\Gamma' \cong \mathbb{C} - L_\rho/L_\rho$ .

Summarizing, we see that while both operations  $F_p$  and  $\sigma_p$  on  $\mathbb{Z}_{\geq 0}$  are given by a concrete rules between integers, only the operation  $f_p$  (inherited from  $F_p$ ) is given by a concrete formula. Each  $p \in \mathcal{P}_S$  arranges the set  $\{c_n, n \geq 0\}$  as step, graded sequences whose all horizontal terms are uniquely determined by the first coefficient of the sequence, whose steps have lenght equal to  $p$  and (for a fixed  $p$ ) are not related to each other by any numerical formula. Moreover, the coefficient  $c_0$  possess a distinguish role in this presentation.

We have seen that for all primes  $p \in \mathcal{P}_S$  the image  $P_p(\tau)$  of each  $G_p(\tau)$  under the Hecke operator  $[\Gamma_0(p)\omega_p\Gamma]_0$  coincide with the sum of the absolute invariant  $j(\tau)$  and the value of the function  $P_p(\tau)$  at the distinguish point  $\rho$ . This determines the unique point  $[\hat{u}_p]_0 \in X_0(p)$ ,  $\hat{u}_p \in R \subset R_p$ , that has the property

$$G_p(\hat{u}_p) = - \sum_{k=0}^{p-1} G_p\left(\frac{\hat{u}_p + k}{p}\right)$$

Moreover, for each such prime (and only for those primes) we may write the Klein modular function  $j(\tau)$  as

$$(4.3) \quad j(\tau) = G_p(\tau) + \sigma_1(\{G_p(\frac{\tau + k}{p}), k = 0, \dots, p-1\}) + j(\hat{u}_p)$$

where  $\sigma_1$  is the standard symmetric function of  $p$  variables. Let us rewrite the last formula (4.3) as follows

$$(4.4) \quad j(\tau) = G_p(\tau) + \sum_{r \in \mathcal{C}_p} G_p\left(\frac{\tau}{p} + r\right) + const, \quad \tau \in H$$

where  $\mathcal{C}_p = \left\langle \frac{1}{p} + L_{\frac{\tau}{p}} \right\rangle$  is a cyclic subgroup of  $p$ -points of the lattice  $[1, \frac{\tau}{p}]$ . This illustrates the fact that the modular invariant  $j(\tau)$  has a hidden,  $p$ -cyclic symmetries which are associated to the modular pairs  $(L_{\frac{\tau}{p}}, \mathcal{C}_p)$  stabilized by  $\Gamma_0(p)$ . So, the expression of the Klein modular function  $j(\tau)$  in terms of the  $\Gamma_0^+(p)$  invariant functions  $G_p(\tau)$  using the appropriate Hecke operators  $[\Gamma_0(p)\omega_p\Gamma]_0$  exhibits a hidden  $p$ -cyclic symmetry which occurs in both, in the formula (4.4) and in the arrangement of the coefficients  $c_n$ 's as  $p$ -step, graded sequences.

We notice that the formula (3.18) for  $P_p(\tau)$  immediately relates this function to the denominator identities of the Monster Lie algebra discovered by Borcherds, [6], and others. These facts together with the relations (obtained when we consider all  $p \in \mathcal{P}_S$  simultaneously) between the coefficients  $c_n \in \{f_p^k(c_m)\}_{k=0}^\infty$  and  $c_{\sigma_p^n} \in \{f_{p_1}^k(c_{m_1})\}_{k=0}^\infty$  for  $p \neq p_1$  indicates that the representation of the full hidden symmetry of  $j(\tau)$  may be given by some sort of a vertex operator algebra.

## 5. CONCLUSIONS

In all three papers, in [4], [5] and in the present one we observe a particular relationship between the modular curve  $Y_0(1) = H/\Gamma$  and the curve  $\mathcal{E} : t^2 = 4u^3 - 1$  analytically isomorphic to the Veech modular curve  $\mathbf{T}^* = H/\Gamma' \cong \mathbb{C} - L_0/L_0$  with  $L_0 \cong L_\rho$ ,  $\Gamma' = [\Gamma, \Gamma]$ . As we have already mentioned, the properties of the Veech modular curve  $\mathbf{T}^*$  produce a generating matrix for the Golay code  $G_{24}$  whose full automorphism group is given by the Mathieu group  $\mathcal{M}_{24}$ . Hence,  $\mathcal{M}_{24}$  must be a subgroup of the full group of hidden symmetries associated to the function  $j(\tau)$ . In this paper we indicate that for each  $p \in \mathcal{P}_S$  function  $j(\tau)$  exhibits a hidden  $p$ -cyclic symmetry coming from the relations between  $j(\tau)$  and  $\Gamma_0^+(p)$ -invariant functions  $G_p(\tau)$ 's and described in the previous section. Hence, the full group of hidden symmetries associated to  $j(\tau)$  contains  $\mathcal{M}_{24}$  and has the order which is divided by all  $p \in \mathcal{P}_S$ . If this group is a simple one it has to be the monster group  $\mathbf{M}$ .

The particular role of the point  $\rho \in H$  revealed in (3.12) and (3.18) is supported by the mentioned above results of [4], [5] as well as by the results of Harada and Lang in [7]. They have shown that the all five curves associated to some special conjugacy classes of the Conway group  $\mathcal{O}$  of all automorphisms of the Leech lattice  $\Lambda$  (which, by the way, originates with  $G_{24}$ ) are elliptic curves that represent the Riemann surface  $\mathbf{T}^*$ , that is, all these curves have the  $j$ -invariant equal to zero.

In our considerations we have assumed that all meromorphic functions  $G_p$  on  $X_0(p)$  are known and we have used them to describe relationships between the coefficients  $c_n$ ,  $n \in \mathbb{Z}^+$  of  $j(\tau)$ . However, as to the author's knowledge, except for  $p = 2, 3, 5, 7$  and 13, when  $G_p(\tau)$  can be written in terms of the absolute invariants  $\Phi_p$  as in (3.6), it is not a case. So, let us reverse the situation. Let us try to find properties of the coefficients  $\alpha_n^p$ 's for  $p = 11, 17, \dots, 71$  and  $n \in \mathbb{Z}^+$ . Since  $c_n \in \mathbb{Z}^+$  we may assume that  $\alpha_n^p = \Omega_n^p + g_n^p$  where  $g_n^p \in \mathbb{Q}$  and  $\Omega_n^p$  is either zero or pure not-rational. When the genus of  $X_0(p)$  is zero then all  $\Omega_n^p = 0$  and all  $\alpha_n^p$  are integers. For the remaining  $p \in \mathcal{P}_S$  it may not be so. However, we immediately obtain that

$$(5.1) \quad \Omega_{pn}^p = -\frac{\Omega_n^p}{p} \quad \text{and} \quad \Omega_{p^k n}^p = (-1)^k \frac{\Omega_n^p}{p^k}$$

Hence, for any  $n = p^l m$  with  $p \nmid m$  i.e. for any  $n \in \{F_p^k(m)\}_{k=0}^\infty$  we have

$$(5.2) \quad \Omega_{p^l m}^p = (-1)^l \frac{\Omega_m^p}{p^l} \rightarrow 0 \quad \text{as } l \rightarrow \infty$$

If  $\Omega_m^p \neq 0$ , ( $p \nmid m$ ) then we will call it the universal  $(p, m)$ -invariant or the universal  $(p, m)$ -constant. Now, what can we find about the pure rational part  $g_n^p$  of  $\alpha_n^p$ ? Let  $g_n^p = \frac{a_n}{b_n}$  with  $\gcd(a_n, b_n) = 1$  and with the obvious upper index  $p$  omitted. From (3.22) we obtain  $a_n b_{pn} + p a_{pn} b_n = b_n b_{pn} c_n$  and hence  $b_n | b_{pn}$  and  $b_{pn} | p b_n$ . For a more general case let us rewrite the formulw (4.1) as

$$(5.3) \quad p^k \alpha_{p^k n}^p + (-1)^{k+1} \alpha_n^p = p^{k-1} c_{p^{k-1} n} - p^{k-2} c_{p^{k-2} n} + \dots + (-1)^{k-1} c_n$$

and let us denote the left side of of this equality by  $A_n^{p,k}$ . Since all of the  $\Omega$ -terms will cancel with each other we will end with

$$a_n b_{p^k n} + (-1)^{k+1} p^k b_n a_{p^k n} = b_n b_{p^k n} A_n^{p,k}$$

Similarly as before, for any  $k \geq 1$ , we must have  $b_n | b_{p^k n}$  and  $b_{p^k n} | p^k b_n$ . There are (a.o.) two simple possibilities: either we have  $b_{pn} = p b_n$  for  $n \in \mathbb{Z}^+$  (and hence  $b_{p^k n} = p^k b_n$ ) or we have  $b_{pn} = b_n$ . In the former case we would obtain

$$G_p(\tau) = q^{-1} + (\Omega_0^p + g_0^p) + \sum_{n \notin (p)} \sum_{k=0}^{\infty} \left[ \frac{\Omega_n^p}{p^k} + \frac{a_{p^k n}}{p^k b_n} \right] q^{p^k n}$$

and in the latter one

$$G_p(\tau) = q^{-1} + (\Omega_0^p + g_0^p) + \sum_{n \notin (p)} \sum_{k=0}^{\infty} \left[ \frac{\Omega_n^p}{p^k} + \frac{a_{p^k n}}{b_n} \right] q^{p^k n}$$

which in a case when all  $\Omega_n^p$  are equal to zero becomes

$$G_p(\tau) = q^{-1} + g_0^p + \sum_{n \notin (p)} \frac{1}{b_n} \sum_{k=0}^{\infty} a_{p^k n} q^{p^k n}$$

In principle, there is nothing in the way for both of the above cases to occur. We may also have a mixed situation when , for example,  $b_{p^3 n} = p b_{p^2 n}$  and  $b_{p^2 n} = b_{pn} = b_n$ , etc. (All of the division conditions stated above can be, in such mixed cases, fulfilled as well.)

Let us say something about the section 2. We have shown that the class number  $h_K$  for  $p \equiv 1 \pmod{4}$  and  $h_K + h_2$  for  $p \equiv 3 \pmod{4}$  is given by the total branch number  $B$  of the mapping  $\pi_\omega : X_0(p) \rightarrow \Sigma \cong X_0(p)/\tilde{\omega}_p$ . This means that it is ruled by the Riemann-Hurwitz formula which, in our case, becomes  $g = 2\gamma - 1 + \frac{B}{2}$  where  $g$  is the genus of  $X_0(p)$ ,  $\gamma$  denotes the genus of  $\Sigma$  and  $B = \sum_{x \in X_0(p)} b(x)$  is always even. (For any  $x \in X_0(p)$  the ramification number is  $r(x) = b(x) + 1$  with  $\sum_{x \in \pi_\omega^{-1}(\varsigma)} r(x) = 2$  for each  $\varsigma \in \Sigma$ ). Thus we have

$$(5.4) \quad h_K = 2g + 2 - 4\gamma \quad \text{and} \quad h_K + h_2 = 2g + 2 - 4\gamma$$

for  $p \equiv 1 \pmod{4}$  and for  $p \equiv 3 \pmod{4}$  respectively. For a prime  $p \in \mathcal{P}_S$  we have  $\gamma = 0$  and the total branching number  $B$  is equal to the cardinality  $2g + 2$  of the set  $\mathfrak{W}_p$  of the Weierstrass points of  $X_0(p)$ .

The Gauss conjecture restricted to the class numbers for imaginary quadratic fields  $K = \mathbb{Q}(\sqrt{-p})$  states that

$$(5.5) \quad h_K \rightarrow \infty \quad \text{as } p \rightarrow \infty$$

and we have found a geometric interpretation of this fact given by the number of the ramification points of the projections  $\pi_\omega$ 's. Since in this case the whole class groups  $Cl_K$  are the principal genus (which tends to be cyclic more often than not [8]) we may approach the open question when  $Cl_K$  is cyclic by looking for the properties of the ramification points of  $\pi_\omega$  on  $X_0(p)$ .

Finally let us list some questions (which may already have nice and simple answers)

- Find the values of  $P_p(\rho)$  for  $p \in \mathcal{P}_S$
- Find  $\hat{u}_p \in R$
- Use the relations between the coefficients  $c_n$  of  $j(\tau)$  and  $\alpha_n^p$  of  $G_p(\tau)$  for all  $p \in \mathcal{P}_S$  (determined in this paper) to find whether this leads to some vertex operator algebra.
- Find whether  $\Omega_n^p = 0$  for all  $p \in \mathcal{P}_S$
- If  $\Omega_n^p \neq 0$  determine whether  $\Omega_n^p = \Omega_m^p$  for  $n, m \notin (p)$ ,  $n \neq m$ . If  $p$  would have such property then we would have (pure not rational) universal  $p$ -constant  $\Omega^p \notin \mathbb{Q}$ .
- Find whether  $b_n \neq 1$  for  $n \notin (p)$
- Find when the class group  $Cl_K$ ,  $K = \mathbb{Q}(\sqrt{-p})$ , is a cyclic one using the properties of the stable points of  $\tilde{\omega}_p$  on  $X_0(p)$ .
- Express the class number  $h_K$  for an arbitrary imaginary quadratic field  $K = \mathbb{Q}(\sqrt{-N})$ ,  $N > 0$ , using the Ogg's results and the Riemann-Hurwitz theorem for the appropriate projections and describe the group properties of  $Cl_K$  using the properties of the ramification points (of these projections) on  $X_0(N)$ .

## REFERENCES

- [1] Ogg, A., *On the Weierstrass points of  $X_0(N)$* , Illinois Journal of Mathematics, **22** (1978), 31-35
- [2] Diamond, F., J. Shurman, *A first course in modular forms*, Springer, 2005
- [3] Silverman, J., *Advanced Topics in the arithmetic of elliptic curves* Springer-Verlag, 1994
- [4] Bugajska, K., *About a moduli space of elliptic curves and the Golay code  $G_{24}$* , submitted for publication
- [5] Bugajska, K., *About some family of elliptic curves*, submitted for publication
- [6] Borcherds, R., *Monstrous moonshine and monstrous Lie superalgebras*, Inventiones Mathematicae, **109**, (1992) 405-444
- [7] Harada, K., M. Lang, *Some elliptic curves arising from the Leech lattice*, Journal of Algebra, **125** (1989) 298-310
- [8] Iwaniec, H., E. Kowalski, *Analytic number theory*, American Mathematical Society, 2004

DEPARTMENT OF MATHEMATICS AND STATISTICS, YORK UNIVERSITY, TORONTO, ON, M3J 1P3  
*E-mail address:* bugajska@yorku.ca